CIV : Application linéaire

Def : Soit $f : E \longrightarrow F$ une app où E et F sont deux K-espace vec. On dit que f est une app linéaire (ou un homomorphisme d'esp vec) si :

- $f(x+y) = f(x) + f(y)$
- $f(\lambda x) = \lambda . f(x)$

$\forall x, y \in E$
$\forall \lambda \in K$

Remarque : Soit $f : E \to F$ une app linéaire

1) On a $f(0) = 0$

Car $f(0) = f(0+0) = f(0) + f(0)$
c'id $f(0) = 0$

2) $f(-x) = f((-1)x)$
$= (-1) f(x)$

$f(-x) = -f(x)$

Def : Soit $f : E \longrightarrow F$ une app linéaire.

1) Si $E = F$, on dit que f est un endomorphisme d'esp vec
Si en plus f est bijective, f est dite un automorphisme d'esp vec

2) On appelle noyau de f, noté $\ker f$, le sous ensemble $\ker f = \{ x \in E, f(x) = 0 \}$

3) On appelle image de f, noté $\mathrm{Im}(f)$, l'ensemble image de f.

$\mathrm{Im}(f) = \{ f(x), x \in E \}$

Prop : Soit $f : E \longrightarrow F$ une app linéaire, Alors on a :

1) $\ker(f)$ est un s.e.v de E
2) $\mathrm{Im}(f)$ " " F

Preuve : 1) * $\ker(f) \neq \emptyset$ Car $0 \in \ker f$

* Soit $x, y \in \ker f$

On a $f(x+y) = f(x) + f(y) = 0$

D'où $x+y \in \ker f$

* Soit $x \in \ker f$ et $\lambda \in K$

On a $f(\lambda x) = \lambda f(x) = \lambda . 0 = 0$

D'où $\lambda x \in \ker f$

Ainsi $\ker f$ est s.e.v de E

2) Dem : $\mathrm{Im} f$ est un s.e.v de F

Théorème : Soit $f : E \to F$ une app linéaire t.q

$\dim E = \dim F$

Alors on a f inj $\Leftrightarrow$ f surj $\Leftrightarrow$ f bij

Preuve : Mq

f inj $\Rightarrow$ f surj $\Rightarrow$ f bij $\Rightarrow$ f inj

* f inj $\Rightarrow$ f surj

$f : E \to F$ est injective

Donc $f_0 : E \to \mathrm{Im}(f)$ est un isomorphisme.

$x \to f(x)$

dont $\dim E = \dim \mathrm{Im} f$

or $\dim E = \dim F$ donc

$\left.\begin{array}{l} \dim \mathrm{Im} f = \dim F \\ \mathrm{Im} f \subseteq F \end{array}\right\} \Rightarrow \mathrm{Im} f = F$

C.à.d f est surjective.

* f surj $\Rightarrow$ f est bij

$\dim \ker f = \dim E - \dim \mathrm{Im} f$ (D'après le thé du rang)

$= \dim E - \dim F = 0$

Donc $\ker f = \{0\}$ Donc f est injective

et donc bijective

* f bij $\Rightarrow$ f inf

Evident

Théorème : (du rang)

Soit $f : E \to F$ une app linéaire, Alors on a

$$\dim \operatorname{Ker} f + \dim \operatorname{Im} f = \dim E$$

On appelle rang de f et on note $rg(f)$, la dimension de $\operatorname{Im}(f)$

$$rg(f) = \dim(\operatorname{Im}(f))$$

Prop : Soit $f : E \to F$ une app lineaire. Alors on a

1) f est surjective $\Leftrightarrow$ $\dim \operatorname{Im} f = \dim F = rg(f)$

2) f est inj $\Leftrightarrow$ $\operatorname{Ker} f = \{0\}$

Preuve : 1) Evident car $\operatorname{Im} f \subseteq F$ $\quad$ $\dim \operatorname{Im} f = \dim F$ et $\operatorname{Im} f \subseteq F \Rightarrow \operatorname{Im} f = F$

2) $\Rightarrow$) Supp que f est injectif et soit $x \in \operatorname{Ker} f$.

On a $\left.\begin{array}{l} 0 = f(x) \\ 0 = f(0) \end{array}\right\} \Rightarrow \left.\begin{array}{l} f(x) = f(0) \\ \text{or } f \text{ inj} \end{array}\right\} \Rightarrow x = 0$

$\Leftarrow$) Supp que $\operatorname{Ker} f = \{0\}$ et soit $x, y \in E$ tq $f(x) = f(y)$

On a $0 = f(x) - f(y) = f(x-y)$

c à d $x - y \in \operatorname{Ker} f = \{0\}$

c à d $x = y$

Donc f est inj

Application :

Soit E, F deux sous espaces vec d'un K-esp. vec L. Alors

On a, $\dim(E+F) = \dim(E) + \dim(F) - \dim(E \cap F)$

Preuve : soit

$$f : E \times F \longrightarrow E + F$$
$$(x, y) \longrightarrow x + y$$

On vérifie que f est une app linéaire surjective.

$$\operatorname{Ker} f = \{(x, y) \in E \times F \,/\, f(x, y) = x + y = 0\}$$

$= \{ (x, -x) / x \in E \cap F \}$

On : $g : \ker f \longrightarrow E \cap F$

$(x, -x) \longrightarrow x$ est un isomorphisme

donc $\dim(\ker f) = \dim(E \cap F)$

Or le théorème du rang montre que

$$\left.\begin{aligned} \dim(E \times F) &= \dim(\ker(f)) + \dim(\mathrm{Im}(f)) \\ &= \dim(E \cap F) + \dim(E + F) \end{aligned}\right\} \Rightarrow$$

Or $\dim(E \times F) = \dim(E) + \dim(F)$

$$\boxed{\dim(E+F) = \dim E + \dim F - \dim(E \cap F)}$$

☺ **Exercice :**

Soit $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$

$(x,y,z) \longrightarrow (x+y, x+y, x+y)$

1) Mq f est une app linéaire.

2) Donner une base de $\ker(f)$

3) Donner une base de $\mathrm{Im}(f)$

4) Mq $\ker f \oplus \mathrm{Im} f = \mathbb{R}^3$

✓ ——

1) Mq f est une app linéaire pour cel

$\forall (x,y,z), (a,b,c) \in \mathbb{R}^3$

* $f((x,y,z) + (a,b,c)) \overset{?}{=} f((x,y,z)) + f((a,b,c))$

$f((x,y,z) + (a,b,c)) = f((x+a, y+b, z+c))$

$= (x+a+y+b, x+a+y+b, x+a+y+b)$

$= (x+y, x+y, x+y) + (a+b, a+b, a+b)$

$f((x,y,z)+(a,b,c)) = f((x,y,z)) + f((a,b,c))$

* $f(\lambda(x,y,z)) \overset{?}{=} \lambda f((x,y,z))$

$f(\lambda(x,y,z)) = f(\lambda x, \lambda y, \lambda z)$

$= (\lambda x + \lambda y, \lambda x + \lambda y, \lambda x + \lambda y)$

$= \lambda(x+y, x+y, x+y)$

$f(\lambda(x,y,z)) = \lambda f((x,y,z))$

Alors f est une application linéaire.

2) On a $\ker f = \{(x,y,z) / (x+y, x+y, x+y) = 0\}$

$= \{(x,y,z) / x+y = 0\}$

$= \{(x,-x,z) / x,y \in \mathbb{R}\}$

C à d $\ker f = \{(x,-x,0) + (0,0,z)\}$

$= \{x(1,-1,0) + z(0,0,1)\}$

$= \langle B \rangle$

tel que $B = \{(1,-1,0), (0,0,1)\}$ un s.e.l

donc $\ker f$ est l'engendré par B

- On a $\forall \alpha, \lambda \in \mathbb{R}$

$\alpha(1,-1,0) + \lambda(0,0,1) = (0,0,0)$

$\Rightarrow (\alpha, -\alpha, \lambda) = (0,0,0)$

$\Rightarrow \alpha = \lambda = 0$

Donc B est libre

Alors B est une base pour $\ker f$

3) On a Thé du rang

$\text{Im } f = \{f((x,y,z)) / (x,y,z) \in \mathbb{R}^3\}$

$= \{(x+y, x+y, x+y) / x,y, \in \mathbb{R}\}$

$= \{(x+y).(1,1,1) / x,y \in \mathbb{R}$

$\text{Im } f = \langle A \rangle$ $A = \{(1,1,1)\}$

Alors A est un système générateur

$\forall a \in \mathbb{R}$ tq

$a(1,1,1) = (0,0,0)$

$\Rightarrow (a,a,a) = (0,0,0)$

$\Rightarrow a = 0$

Donc A est un S libre

Alors A est une base de $\text{Im } f$

Prop : Soit $f : E \to F$ une app linéaire avec $B = (e_1, e_2, \dots, e_n)$ une base de E

Alors : $\mathrm{Im} f = \langle \{ f(e_1), \dots, f(e_n) \} \rangle$

Car : $\mathrm{Im}(f) = \{ f(x) \ / \ x \in E \}$

$= \{ f(\sum_{i=1}^{n} \lambda_i e_i) \ / \ \lambda_i \in \mathbb{K} \}$

$= \{ \sum_{i=1}^{n} \lambda_i f(e_i) \ / \ \lambda_i \in \mathbb{K} \}$

$= \langle \{ f(e_1), \dots, f(e_n) \} \rangle$

Remarque : soit $f : E \longrightarrow F$ app linéaire

$B = (e_1, \dots, e_n)$ une base de E

Déterminer $f \Leftrightarrow$ déterminer $\{ f(e_1), \dots, f(e_n) \}$

$\Rightarrow$ f v. dont.

$\Leftarrow$ Soit $x = \sum_{k=1}^{n} \lambda_i a_i \in E$

$f(x) = \sum_{i=1}^{n} \lambda_i f(a)$

Ex :

Dans $\mathbb{R}^2$, si $e_1 = (1,0)$, $e_2 = (0,1)$

$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$f(e_1) = (1,1)$

$f(e_2) = (1,-1)$

$f(x,y) = f(x e_1 + y e_2)$

$= x f(e_1) + y f(e_2)$

$f(x,y) = (x+y, x-y)$

Matrice

Def :

Une matrice est un tableau rectangulaire d'éléments de $K (K = \mathbb{R}, \mathbb{C})$ qui a n lignes et m colonnes

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \cdots & a_{ij} & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

avec a_{ij} est l'intersection de la i-ème colone et le j ème ligne.

L'ensemble des matrices de ce type (n, m) est noté $M_{nm}(K)$

Dans $M_{nm}(K)$, on définit une loi de composition interne noté "+" et définie par

si $A = (a_{ij})_{ij}$ $\quad B = (b_{ij})_{ij}$

On a $A + B = (a_{ij} + b_{ij})$

$(M_{nm}(K), +)$ est un groupe commutatif avec comme élément neutre la matrice nulle

$A = (a_{ij})_{ij}$ avec $\forall i,j \; a_{ij} = 0$

Le symétrique de la matrice $A = (a_{ij})_{ij}$ est la matrice noté $(-A)$ et définie par $(-A) = (-a_{ij})_{ij}$

On définit aussi sur $M_{ij}(K)$ une loi de composition interne définie par :

si $\lambda \in K$ et $A = (a_{ij})_{ij}$

On a $\lambda A = (\lambda a_{ij})_{ij}$

On vérifie que $(M_{n,m}, +, \cdot)$ est un K-esp-vect

$M_{n,m}(K) = \{ A = (a_{ij}) / \quad \} = \{ \sum a_{ij} E_{ij} / \; i = \overline{1,n} \}$

$M_{n,m}(K) = \langle \{E_{ij}\} \rangle$

4) Mq E est un corps

✓

Soit $E = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} / a, b \in \mathbb{R} \right\}$

1) $M_2(\mathbb{R})$ est esp-vec et $E \subseteq M_2(\mathbb{R})$

Il suffit de montrer que E est un s.e.v de $M_2(\mathbb{R})$

On a $E = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} / a, b \in \mathbb{R} \right\}$

$= \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} / a, b \in \mathbb{R} \right\}$

$= \left\langle \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \right\rangle$

$= \langle \{I, L\} \rangle$

$E = \langle S \rangle$

donc E est un s.e.v de $M_2(\mathbb{R})$ donc e.v

S est un système générateur on vérifier si il est libre.

Soit $\alpha, \beta \in \mathbb{R}$ tq $\alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\Rightarrow \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\Rightarrow \alpha = \beta = 0$

d'où S est libre

donc S est une base de E et $\dim(E) = \text{card}(S) = 2$

3) $L^2 = L \times L = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$= -I_2$

donc $(-L) \times (L) = I_2$ d'où L est inversible.

et $L^{-1} = -L$

4) Mq E est un corps, $E \subseteq M_2(\mathbb{R})$

- Mq (.) est commutative
- Mq $\forall A \in E$ tq $A \neq 0$ A est inversible.

Système linéaire

☺ **Def :** Soit $A \in M_{mn}(\mathbb{K})$ une matrice, on dit que A est échelonnée réduite ligne, si le nombre de zéro successif de chaque ligne de la gauche à la droite est strictement croissant et que le premier élément non nul de la gauche de chaque ligne non nulle est 1

☺ **exemple :**

1) $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ est échelonnée réduite ligne.

2) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ est n'est pas e.r.l

3) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ est n'est pas e.r.l

☺ **Exemple :**

Résoudre le système linéaire suivant :

1- (S_1) : $\begin{cases} x + y + z = 1 \\ x - y + z = 2 \\ x + z = 0 \end{cases}$

✓ La matrice associé à (S) est la matrice A donnée par

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$\sim$ $L_2 - L_1$, $L_3 - L_1$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & 1 \\ 0 & -1 & 0 & -1 \end{pmatrix}$$

$\sim$ $L_{2,3}$ permutation

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & -1 \\ 0 & -2 & 0 & 1 \end{pmatrix}$$

$\sim$ $(-1)L_2$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & & & \end{pmatrix}$$

$\sim$ ($L_3 \leftarrow L_3 + L_2$)
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$\sim$ ($\left(\frac{1}{3}\right) L_3$)
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Donc On a

$$\begin{cases} 0x + 0y + 0z = 1 \\ 0x + y + 0z = 1 \\ x + y + z = 1 \end{cases} \Rightarrow \begin{cases} 0 = 1 \\ y = 1 \\ x + y + z = 1 \end{cases}$$

$S = \emptyset$

2- S_2
$$\begin{cases} x + y - z = 1 \\ x - y - z = 2 \\ x + y + z = 0 \end{cases}$$

La matrice associé à (S) est la matrice A donnée par :

$$A = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 2 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$\sim$ ($L_2 \leftarrow L_2 - L_1$, $L_3 \leftarrow L_3 - L_1$)
$$\begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & -1 \end{pmatrix}$$

$\sim$ ($\left(-\frac{1}{2}\right) L_2$, $\left(\frac{1}{2}\right) L_3$)
$$\begin{pmatrix} 1 & 1 & -1 & 1 \\ 0 & 1 & 0 & -\frac{1}{2} \\ 0 & 0 & 1 & -\frac{1}{2} \end{pmatrix}$$

Donc

$$(S) : \begin{cases} 0x + 0y + z = -\frac{1}{2} \\ 0x + y + 0z = -\frac{1}{2} \\ x + y - z = 1 \end{cases} \Rightarrow \begin{cases} z = -\frac{1}{2} \\ y = -\frac{1}{2} \\ x = 1 \end{cases}$$

$$\Rightarrow S = \left\{ \left(1, -\frac{1}{2}, -\frac{1}{2}\right) \right\}$$

3- S_3
$$\begin{cases} -x + y + z = 1 \\ x - y + z = 1 \\ x - y = 0 \end{cases}$$

☺ **Système de Cramer :**

Soit un système linéaire

$$\begin{cases} a_1 x + a_2 x + a_3 x = d_1 \\ b_1 x + b_2 x + b_3 x = d_2 \\ c_3 x + c_2 x + c_1 x = d_3 \end{cases}$$

Posons

$$B = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}$$

et $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ et $D = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \end{pmatrix}$

On a $BX = D$

si B est inversible, on dit que le système est de Cramer, Dans ce cas on a

$$X = B^{-1} D$$

et (S) admet une solution unique.

Chapitre 1 : Arithmétique

I - Division euclidienne dans $\mathbb{Z}$:

Proposition : Soient a et $b \in \mathbb{Z}$ avec $b > 0$. Il existe un couple unique d'entiers q et r tel que $\boxed{a = qb + r}$ avec $\boxed{0 \leq r < b}$ q est appelé le quotient et r le reste de division euclidienne de a par b.

Preuve : Notons par q la partie entière de $\boxed{\frac{a}{b}}$

$q = E\left(\frac{a}{b}\right)$ on a $q \leq \frac{a}{b} < q+1$

et par suite on a $bq \leq a < bq + b$

C'est à dire $0 \leq a - bq < b$

de sorte qu'il suffit de prendre $r = a - bq$

* si deux couple (q, r) et (q', r') satisfont les mêmes conditions c'est à dire $\begin{cases} r = a - bq \\ r' = a - bq \end{cases}$

$\Rightarrow bq - bq' = r' - r \Leftrightarrow b(q - q') = r' - r$

or $\begin{matrix} 0 \leq r < b \\ 0 \leq r' < b \end{matrix} \Rightarrow |r - r'| < b$

$\Rightarrow b|q - q'| = |r' - r| < b$ car $0 < b$ ..

$\Rightarrow \left.\begin{matrix} |q - q'| < 1 \\ |q - q'| \in \mathbb{N} \end{matrix}\right\} \Rightarrow q - q' = 0$

C'est à dire $\boxed{q = q'}$

D'où $r' - r = b(q - q') = 0$

C'est à dire $\boxed{r' = r}$

Exemple :

$\frac{11}{2} = \frac{5}{q} \times \frac{2}{b} + \frac{1}{r}$

$\begin{matrix} 11 \\ 10 \\ 01 \end{matrix} \Big| \begin{matrix} 2 \\ 5 \end{matrix}$

II - Congruence modulo $n \in \mathbb{Z}$:

Def: Soit n un entier naturel $(x, y) \in \mathbb{Z}^2$

on dit que x si congru à y modulo n

si $x - y \in n\mathbb{Z}$ c'est à dire $\boxed{x = y + kn}$

avec $\boxed{k \in \mathbb{Z}}$

on écrit alors $x \equiv y$ (modulo n) ou simplement

$x \equiv y\ [n]$

On définit la classe de modulo n, noté par $\bar{x}$ ou $c(x)$, comme suit:

$$\bar{x} = x + n\mathbb{Z} = \{x + kn \ / \ k \in \mathbb{Z}\}$$

Cas particulier :

① $n = 2$

Il ya deux classes:

$\bar{0} = \{\dots, -2, 0, 2, 4 \dots\}$

$\bar{1} = \{\dots, -1, 1, 3, \dots\}$

Aussi $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

② $n = 3$

$\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$

III - pgcd, ppcm et nombre premier :

1-Divisibilité :

Soit $a, b \in \mathbb{Z}^*$. On dit que b divise a s'il existe $c \in \mathbb{Z}$ tel que $a = bc$. On note $b \mid a$,

si $a \mid b$ et $b \mid a$, alors $\exists\, c, c'$ tel que $b = ac$ et $a = bc'$

D'où $b = ac = bcc'$

c'est à dire $cc' = 1$

c'est à dire $c = c' = \pm 1$

Aussi $a = \pm b$ a et b sont dits associés

Defi Les éléments $p \in \mathbb{Z} - \{-1, 1\}$ qui admettent pour seuls diviseurs $\pm p$ et ± 1, sont dit **des nombres premiers**.

En general, on parlera des nombres premiers > 0

Proposition: Tout entier est produit de facteurs premiers.

Preuve: Par récurrence.

Proposition: L'ensembles des nombre premier est infini

Preuve: Supposons que l'ensemble de nombre premier est fini, soit $\{P_0, P_1 \dots P_n\}$ l'ensemble de ces nombres premiers

Posons $P = \prod_{i=1}^{n} P_i$ et $N = P + 1 > P_i \ \forall i \dots$

Comme N ne peut pas être un nombre premier

$\exists i = 1, \dots n$ tel que $\left.\begin{matrix} P_i \mid N \\ \text{or} \quad P_i \mid P \end{matrix}\right\} \Rightarrow P_i \mid N - P$

c à d $P_i = 1$ absurde

Donc l'ensemble des nombres premiers est infini.

2 - Pgcd:

Def soit $a, b \in \mathbb{N}^*$. Le p.g.c.d de a et b noté $a \wedge b = d = pgcd(a, b)$ est l'entier $d \in \mathbb{N}^*$

tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Preuve:

* $a = a \cdot 1 = a \cdot 1 + b \cdot 0$

$\in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

d'où $d \mid a$

* $b = a \cdot 0 + b \cdot 1$

$\in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

et donc $d \mid b$

* Soit $h \in \mathbb{N}^*$ tel que $\begin{cases} h/a \\ h/b \end{cases}$

c'est à dire $\exists (k, \ell) \in \mathbb{N}^{*2} / \begin{cases} a = hk \\ b = h\ell \end{cases}$

$$d = d.1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$$
$$\supset hk\mathbb{Z} + h\ell\mathbb{Z}$$
$$\subset h\mathbb{Z}$$

d'où h/d

Aussi d est le plus grand commun diviseur de a et de b.

Calcul de pgcd (Algorithme d'Euclide):

On suppose que $a > b \neq \mathbb{Z}$ et $b \neq 0$ / (sinon, on permute a et b)

on definit par récurrence une suite d'entiers r_k en posant $r_0 = a$, $r_1 = b$ et si $k \geq 1$, et si $r_k \neq 0$, r_{k+1} est le reste de division Euclidienne de r_{k-1} par r_k

$$r_{k-1} = r_k q_k + r_{k+1}$$

avec $0 \leq r_{k+1} < r_k$

si $r_k = 0$, on arrêt.

Le pgcd est donc le dernier reste non nul

Exemple: Posons

$a = 2652$ et $b = 2310$

Les divisions euclidiennes successives donnent

$2652 = 2310 + 342$

$2310 = 342 \times 6 + 258$

$342 = 258 + 84$

$258 = 84 \times 3 + 6$

$84 = 6 \times 14 + 0$

$\boxed{pgcd(a,b) = 6}$

Proposition (l'identité de Bezout).

Soient $a, b \in \mathbb{Z}$ et $d = p.g.cd(a,b) = a \wedge b$

Il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = d$

Preuve: On a $d.1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ et donc

$\exists u, v \in \mathbb{Z}$ tel que $d = ua + vb$

Déf Deux entiers $a, b \in \mathbb{Z}$ sont dits premiers entre eux si $d = pgcd(a,b) = 1 = a \wedge b$

Prop: Deux entiers a et b premiers entre eux si et seulement $\exists u, v \in \mathbb{Z}$ tel que $au + bv = 1$

Prop: (Lemme de Gauss)

Soient $a, b, c \in \mathbb{Z}^*$, si $\left.\begin{array}{l} a/bc \\ \text{et } a \wedge b = 1 \end{array}\right\} \Rightarrow a/c$

Preuve:

Comme $a \wedge b = 1$, $\exists u, v \in \mathbb{Z}$ tel que $au + bv = 1$

on a donc $auc + bvc = c$

et comme $\left.\begin{array}{l} a/bc \\ \text{et } a/auc \end{array}\right\} \Rightarrow \left.\begin{array}{l} a/bc \\ a/c - buc \end{array}\right\} \Rightarrow \left.\begin{array}{l} a/buc \\ a/c - buc \end{array}\right\} \Rightarrow a/c$

3- P.P.C.M:

on dit que m est le plus commun multiple ...

pp cm de a et $b \in \mathbb{N}^*$

si m est un multiple de a et de b tout multiple de a et de b est multiple de m

On écrit $m = ppcm(a,b)$

→ Notons que si $a, b \in \mathbb{N}^*$

on a $pgcd(a,b) \times ppcm(a,b) = ab$

En général : $[a \wedge b] \times [a \vee b] = |ab|$

Chapitre 2 Structure Algébrique

I - Relation d'équivalence :

Définitions: Soit E un ensemble et R une relation sur E

1) On dit que R est **réflexive** si $\forall x \in E \quad x R x$

2) On dit que R est **symétrique** si $\forall x, y \in E$

on a $x R y \Rightarrow y R x$

3) On dit que R est **transitive** si $\forall x, y, z \in E$ on a

$$\left.\begin{array}{l} x R y \\ y R z \end{array}\right\} \Rightarrow x R z$$

4) On dit que R est une relation d'équivalence si R est réflexive, symétrique et transitive

Exemples:

1) Dans un lycée, la relation entre les élèves suivants: "deux élèves sont en relation" si ils ont le même niveau" est une relation d'équivalence.

2) $x \leq y$ n'est pas une relation d'équivalence car elle n'est pas symétrique (car par exemple $1 \leq 2$ mais $2 \not\leq 1$).

Définition:

Soit R une relation dans un ensemble E.

1) On dit que R est est **antisymétrique** si $\forall (x, y) \in E^2$

on a $\left.\begin{array}{l} x R y \\ y R x \end{array}\right\} \Rightarrow x = y$

2) On dit que R est une relation d'ordre si R est réflexive, antisymétrique et transitive.

Exemples:

1) Dans $\mathbb{R}$, la relation $x \leq y$ est une relation d'ordre

2) Dans un ensemble E, la relation d'égalité est une relation d'ordre et d'équivalence.

3) Dans $\mathbb{N}^*$, la relation "$a|b$" est une relation d'ordre.

Prop soit $\mathcal{R}$ une relation dans une ensemble E, Alors ($\mathcal{R}$ est une relation d'équivalence et d'ordre) $\Leftrightarrow$ $\mathcal{R} = (=)$

Preuve $\Leftarrow$ Evident

$\Rightarrow$ Soit $\mathcal{R}$ une relation d'équivalence et d'ordre.

On doit montrer que $\mathcal{R} = =$ C'àd $\forall x,y \in E$

$x \mathcal{R} y \overset{?}{\Leftrightarrow} x = y$

$\Leftarrow$ Evident car $\mathcal{R}$ est reflexive.

$\Rightarrow$ supposons que $x \mathcal{R} y$

Alors $y \mathcal{R} x$ car $\mathcal{R}$ est symétrique

$x \mathcal{R} y$

$\Rightarrow x = y$ car $\mathcal{R}$ est antisymétrique

D'où le resultat.

Definition soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E et soit $x \in E$. La classe d'équivalence de x noté $C(x)$ ou parfois $\bar{x}$, est l'ensemble $C(x) (= \bar{x}) = \{y \in E / x \mathcal{R} y\}$

Exemple:

Soit $n \in \mathbb{Z}^*$ la relation dans $\mathbb{Z}$ defini par :

$x \mathcal{R} y \in \left[\exists k \in \mathbb{Z} / x - y = kn \right]$.

$\Leftrightarrow n / x - y$

1) $\mathcal{R}$ est une relation d'équivalence car

* Réflexivité: $\forall x \in \mathbb{Z}$

on a $x - x = 0 = 0.n$

et donc $x \mathcal{R} x$

* Symétrie: si $x, y \in \mathbb{Z}$ tel que $x \mathcal{R} y$ (à d $x - y = kn$ avec $k \in \mathbb{Z}$ alors $y - x = n(-k)$

et donc $y \mathcal{R} x$

* Transitivité: soit $(x,y,z) \in \mathbb{Z}$ tel que $x \mathcal{R} y$ et $y \mathcal{R} z$

on a $x \mathcal{R} y \Rightarrow \exists k \in \mathbb{Z} / x - y = kn$

$y \mathcal{R} z \Rightarrow \exists l \in \mathbb{Z} / y - z = ln$

d'où $x - z = x - y + y - z = (k+l)n \in \mathbb{Z}$

d'où $x R z$

Donc R est une relation d'équivalence. Cette relation s'appelle relation de congruence modulo n

et noté par $x R y \Leftrightarrow x \equiv y [n]$

On a $n - 0 = 1 . n$ càd $n \equiv 0 [n]$

càd $C(n) = C(0)$

càd $\bar{n} = \bar{0}$

D'où $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est l'ensemble des classes de $\mathbb{Z}$ modulo n.

Définition

Soit R une relation d'équivalence sur un ensemble des classes d'équivalence noté E/R est définie par $E/R = \{C(x) / x \in E\}$ est dit l'ensemble quotient

Dans l'exemple précédent $\mathbb{Z}/R$ est noté $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

Proposition, Soit R une relation d'équivalence sur un ensemble E alors on a

1) $E = \bigcup_{x \in E} C(x)$

2) Soit $x, y \in E$ alors on a

$C(x) \neq C(y) \Rightarrow C(x) \cap C(y) = \emptyset$

Preuve

1) Par définition $C(x) \subseteq E$ et donc $\bigcup_{x \in E} C(x) \subseteq E$

Inversement, soit $y \in E$

$y \in C(y)$ (car R est reflexive $y R y$)

$\subseteq \bigcup_{x \in E} C(x)$

d'où $E = \bigcup_{x \in E} C(x)$